Declaración de privacidad y seguridad

MEIK LABS · Licitación 1016-11-LE26 · Ministerio de Obras Públicas · versión congelada v1.1.0 · generado el 07-11-2026

Producto: ProcesIA · **Oferente:** MEIK LABS
Licitación: 1016-11-LE26 — Dirección de Planeamiento, MOP
Versión: 1.0 (oferta) · **Fecha:** 05-11-2026

> Documento público. Aplica a la solución ofertada y se verificará en las pruebas de aceptación y de seguridad de los numerales 2.8 y 2.12 de las Bases Técnicas.

1. Dónde residen los datos

La solución se instala y opera íntegramente en la máquina virtual del Ministerio (RO-13, RO-14). Todos los datos permanentes —insumos, transcripciones, diagramas, documentos, matrices, versiones, registros de auditoría y respaldos— residen en esa VM, en volúmenes cifrados, y no se replican fuera de ella. MEIK LABS no mantiene copias de la información del Ministerio.

2. Qué se envía fuera de la VM

Solo las solicitudes a los servicios gestionados de la cuenta AWS institucional del Ministerio: transcripción de audio y generación con modelos de lenguaje (RO-15). Se envía únicamente el contenido necesario para cada solicitud —el segmento de audio o el texto del insumo correspondiente— junto con la instrucción acotada de esa tarea. La región y los modelos son los que el Ministerio autorice por escrito y quedan registrados en el diseño detallado; no se habilitan otros sin esa autorización (2.12 a). No se envían credenciales del Ministerio, ni el modelo de datos completo, ni información de un proceso al procesar otro.

3. Entrenamiento de modelos y telemetría

La información del Ministerio no se utiliza para entrenar ni mejorar modelos, ni propios ni de terceros (RO-15, 2.13). La configuración de los servicios se fija para impedir ese uso. La solución no incorpora telemetría, analítica de uso ni servicios de terceros distintos de los autorizados. El mecanismo de licenciamiento valida en forma local y no transmite documentos, grabaciones, transcripciones, instrucciones ni contenido operacional (RO-18).

4. Insumos temporales en la nube

Si la transcripción requiere almacenamiento de objetos temporal, el objeto se elimina automáticamente al completar el flujo y una política de ciclo de vida elimina cualquier residuo en un plazo máximo de 24 horas (RO-16). El borrado se verifica en las pruebas de aceptación y puede ser auditado por el Ministerio durante la vigencia (2.12 c).

5. Personas

La solución no incluye ni habilita identificación de personas por su voz o imagen (RO-01). Las transcripciones distinguen hablantes de forma genérica ("Hablante 1", "Hablante 2") y los roles del proceso se registran por cargo, no por nombre de persona. Cuando un insumo contiene datos personales, el usuario puede marcarlo por actividad (RD-06) y la configuración de enmascaramiento permite ocultar RUT, teléfonos, correos y nombres de terceros antes de enviar contenido a los servicios de inferencia (RD-13).

6. Revisión humana

Todo resultado generado con IA es un borrador sujeto a revisión humana (RO-07, 2.13). Cada artefacto así generado se identifica como borrador, avanza por estados de revisión con registro de autor y fecha (RD-15, RO-08) y requiere validación del dueño o dueña del proceso. La plataforma no adopta decisiones automatizadas respecto de personas.

7. Acceso, trazabilidad y conservación

Los accesos usan el inicio de sesión institucional (RO-11) y cuentas de edición, visualización y administración (RO-10), con credenciales de mínimo privilegio. Cada acceso, modificación y eliminación queda en un registro de auditoría de solo inserción (RO-08). Los plazos de conservación se configuran por tipo de insumo, con eliminación automática o asistida y búsqueda y borrado por persona (RD-16). Al vencer la licencia, la plataforma pasa a solo lectura y exportación sin eliminar ni retener la información (RO-19, RD-11).

8. Seguridad de la infraestructura

Comunicaciones cifradas con TLS 1.2 o superior y respaldos cifrados en reposo (RO-21); análisis antimalware de todo archivo cargado (RO-22); notas de versión y escaneo de vulnerabilidades de componentes en cada release, sin críticas abiertas (RO-23); corrección sin costo de vulnerabilidades críticas y altas en los plazos comprometidos (RO-24). Las conexiones salientes de la VM se limitan a los destinos declarados en la oferta. MEIK LABS acepta las pruebas de seguridad del numeral 2.12, incluidas las de inyección de instrucciones a través de los insumos y de exfiltración de información en las salidas.

9. Portabilidad y salida

El Ministerio puede exportar en cualquier momento, sin costo, la totalidad de su información en los formatos del RO-20, incluidos los registros de auditoría. Al término del contrato, MEIK LABS entrega la exportación final con verificación de integridad, elimina cualquier dato o respaldo en su poder y lo certifica por escrito dentro de los plazos del numeral 2.14.

10. Incidentes

MEIK LABS actúa como encargado del tratamiento respecto de los datos personales a los que acceda y notifica los incidentes de ciberseguridad en el plazo y la forma del Anexo N°3. Los accesos remotos son nominativos, registrados y de mínimo privilegio, por VPN institucional.

Contacto: soporte@meiklabs.com · MEIK LABS, Santiago de Chile.